Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Canceled)

2. (Currently amended) The method as defined in claim 11 [[1]], wherein the sequence number is transmitted together with the signing key from the control center to the sender, and is transmitted from the sender via the data set to the receiver.

3. (Currently amended) The method as defined in claim 11 [[1]], wherein the sequence numbers are used to produce signing keys in the control center and corresponding checking keys in the receiver.

4. (Currently amended) The method as defined in claim 11 [[1]], wherein the sequence numbers are used to produce signing keys used in the control center and corresponding check keys are used in the receiver wherein the sequence number is transmitted via the data set to the receiver.

5. (Currently amended) The method as defined in claim 11 [[1]], wherein the sequence number is produced by a pseudo-random number generator.

6. (Currently amended) The method as defined in claim 11 [[1]], wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

7. (Currently amended) The method as defined in claim 11 [[1]], wherein the control center produces a number of signing keys , and transmits them to the sender, either separately or together with the associated sequence numbers.

8. (Currently amended) The method as defined in claim 11 [[1]], wherein the receiver maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. (Currently amended) A device for signing a message which is sent from a sender to a receiver comprising:

a control center having a first memory and a receiver having a second memory for a secret, common main key;

[[in]] the control center including, one input of a first one-time encrypter being connected to the first memory of the control center, and another input being connected to a generator for a sequence number,

an output of the first one-time encrypter being connected to the sender via a transport medium;

a signature generator provided in the sender, and having inputs connected to the output of the first one-time encrypter and to the message to be signed;

an output of the signature gencrator being connected to a device which assembles at least the signature and the message to form a data message block and whose output is connected to the receiver via a transport medium;

a signature checker is provided in the receiver having inputs connected to the message and to the signature of the data message block which has arrived via the transport medium, and wherein

the inputs of the signature checker are further connected to an output of a second one-time encrypter, whose inputs are connected to the second memory of the receiver for the secret main key and to a means for providing a sequence number .

PAGE 3/20 * RCVD AT 4/8/2005 2:01:41 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID: * DURATION (mm-ss):05-38

10. (Previously Presented) The device as defined in claim 9, wherein the generator to produce a sequence number uses a deterministic method to produce one or more sequence numbers that correspond to the same number of check keys.

11. (Currently Amended) A method for signing a message from a sender and for checking a signature at a receiver, the method comprising the steps of:

initializing ~~providing~~ a control center, ~~a sender~~ and a receiver with a shared main key ~~wherein the control center and the receiver share an undiscoverable main key~~;

causing the control center to produce one or more sequence numbers;

using one of the sequence numbers and the ~~common~~ shared main key to create a signing key by means of a one-time encryption;

providing the signing key and the sequence number to the sender via a secure transmission;

the sender using the signing key to form a signature for a message ~~and sending the message to the receiver via a data set containing at least the message and the signature~~;

the sender forming a data set;

the sender sending the message to the receiver via the data set containing at least the message and the signature;

determining the sequence number from the received data set;

passing the sequence number through a one-time encryption to produce a check key; and

using the check key to verify the signature ~~on the message~~.

PAGE 4/20 * RCVD AT 4/8/2005 2:01:41 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID: * DURATION (mm-ss):05-38